Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2015–2016

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 379

BRIEF VAN DE MINISTER VAN BINNENLANDSE ZAKEN EN KONINKRIJKSRELATIES

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 14 december 2015

Naar aanleiding van het Algemeen Overleg met de Vaste Kamercommissie van BZK van 25 november 2015 en de ingediende moties tijdens het Verslag Algemeen Overleg (VAO)(Handelingen II 2015/16, nr. 34) – en de ingediende moties tijdens het VAO van 8 december 2015 – informeer ik uw Kamer nader over het doel van de pilots met publieke en private middelen voor elektronische identificatie en authenticatie, alsmede over de samenhang tussen de diverse pilots.
In bijlage I geef ik u de informatie waar u in het Algemeen Overleg van 25 november om heeft gevraagd. Het moet duidelijk zijn op welke wijze alle aangekondigde pilots in het publieke domein samenhangen: wat zijn de eenduidige toelatingseisen, wat zijn de eenduidige evaluatiecriteria en welke pilots worden geëvalueerd door de begeleidingscommissie. In het verlengde daarvan is gebleken dat de ministeriële verantwoordelijkheid eenduidiger belegd dient te worden. Conform hetgeen ik u in het Algemeen Overleg meldde, heb ik de situatie in het Kabinet besproken. De uitkomsten daarvan treft u aan in deze brief, die ik u mede namens de Minister van Economische Zaken en de Staatssecretaris van Financiën aanbied. In overeenstemming met de wens van uw Kamer is in het Kabinet besloten om burger-authenticatie in het publieke domein (BSN-domein) via een eenduidiger verantwoordelijkheidstoedeling in te richten.

Doelstelling

In het regeerakkoord is de doelstelling opgenomen dat burgers en bedrijven in 2017 digitaal zaken met de overheid moeten kunnen doen. Daarom kiest het kabinet voor één regime voor identificatie en authenticatie als een belangrijke randvoorwaarde van Digitaal 2017. In het kabinet is nogmaals benadrukt dat beschikbare en betrouwbare authenticatiemiddelen in het burgerdomein van groot en urgent maatschappelijk belang zijn. Belangrijkste redenen hiervoor zijn, dat burgers op een eenvoudige en betrouwbare wijze met één of meer hoogwaardige authenticatiemid-

kst-26643-379
ISSN 0921 - 7371
's-Gravenhage 2015

delen moeten kunnen inloggen bij de overheid en tevens dienstaanbieders in het publieke domein niet afhankelijk mogen zijn van een enkel inlogmiddel. Door deze zogenaamde «multimiddelen-benadering» wordt de afhankelijkheid van DigiD (thans 12 miljoen gebruikers) beperkt.

Eenduidige verantwoordelijkheid

Met u is het kabinet van mening dat de huidige situatie complex is en dat rollen en verantwoordelijkheden eenduidig moeten zijn. Dat is om voldoende vaart te maken met de introductie van meerdere authenticatiemiddelen in het publieke domein. Voor het publieke domein ga ik de regelgeving onder één regime brengen: wettelijke eisen waaraan alle authenticatiemiddelen moeten voldoen voor gebruik in het publieke domein, alsook waaraan alle betrokken partijen moeten voldoen. Het voorgaande zal onderdeel uitmaken van de Wet generieke digitale infrastructuur (Wet GDI), die eerder is aangekondigd.[1] Vanzelfsprekend worden bij de totstandkoming van de eisen – zoals gebruikelijk is bij de voorbereiding van wetgeving – belanghebbende partijen, waaronder middelenleveranciers en dienstverleners, betrokken.
In overleg met mijn collega van Economische Zaken en de Staatssecretaris van Financiën is vastgesteld dat de verantwoordelijkheid voor dit publieke regime bij de Minister van BZK ligt.

Betekenis voor de pilots en samenhang

Het uniform eisenpakket voor de toelating tot de pilots ziet er in hoofdlijnen als volgt uit:

- Betrouwbaarheidsnormen voor het registratie- en uitgifteproces voor een authenticatiemiddel. Dit zijn normen die identiteitsfraude tegengaan, bijvoorbeeld doordat de initiële identiteit van de gebruiker via een face-to-face proces aan de hand van een geldig identiteitsdocument wordt geverifieerd. Toegang kan alleen worden verleend met middelen op een hoog betrouwbaarheidsniveau. Voor betrouwbaarheidsniveaus wordt de Europese eIDAS verordening gehanteerd, welke leidend is voor de invulling hiervan.[2]
- Informatiebeveiligingsnormen, bijvoorbeeld verplichte versleuteling, eisen aan de opslag van persoonsgegevens en dataminimalisatie. Dit zijn tevens maatregelen die bijdragen aan het afschermen van persoonsgegevens en derhalve privacy beschermende maatregelen.
- Privacy beschermende maatregelen: maatregelen over het verzamelen van het inloggedrag van een gebruiker en het geven van inzage recht. Voor de pilots dient een Privacy Impact Analyses (PIA) te zijn uitgevoerd, waarbij getoetst is aan feitelijke en technische nationale en Europese juridische vereisten betreffende privacy.
- Technische eisen: de specificatie van de technische koppelvlakken om te kunnen inloggen in het publieke domein.

De pilots vallen uiteen in drie groepen: (1) pilots met publieke middelen met regelgeving vanuit BZK, (2) pilots met private middelen in het publieke domein op basis van het afsprakenstelsel Idensys, en (3) pilots met bankmiddelen met DNB regelgeving.

---

[1] Laatstelijk in de Uitgangspuntenbrief WGDI dd 4 dec. 2015.

[2] De eIDAS verordening kent drie betrouwbaarheidsniveaus: laag, substantieel en hoog, waarbij tijdens het vaststellen van de eisen die eraan gesteld zijn rekening gehouden is met de betrouwbaarheidsniveaus uit STORK en ISO 29115; zie UITVOERINGSVERORDENING (EU) 2015/1502 VAN DE COMMISSIE van 8 september 2015. Klik hier voor de link.

Alle pilots hebben met betrekking tot de toelatingseisen een adequate invulling:

- De pilots met private middelen (Idensys en banken) hebben gemeen dat ze gebruik maken van een publieke, reeds gereguleerde voorziening, het BSN-koppelregister, waardoor authenticatiemiddelen in het publieke domein kunnen worden gebruikt.
- Zowel de pilots met publieke middelen als met private middelen zijn voor wat het gebruik van BSN betreft wettelijk ingekaderd.[3] Kern van de pilots is dat wanneer partijen aantoonbaar aan de gestelde eisen voldoen, de betreffende middelen worden geaccepteerd in het publieke domein.

Alle pilots worden door een commissie onder het voorzitterschap van dhr. P.W.A. Veld geëvalueerd en daarbij worden dezelfde evaluatiecriteria gehanteerd.[4]

Hoofdlijnen uniform toelatingsstelsel

Er is in de structurele situatie wel een uniform toelatingsstelsel nodig voor het publieke domein waar een eenduidig certificeringsstelsel en toezichtsarrangement onderdeel van uitmaken. In bijlage II treft u een uitwerking op hoofdlijnen aan. Het betekent dat de toelatingseisen voor het eenduidige publieke regime bij elkaar gebracht worden, resulterend in een vastlegging in regelgeving voor het publieke domein (wettelijk regime, de toekomstige wet GDI) onder mijn verantwoordelijkheid.
Het certificeringsstelsel bevat criteria onder andere op het gebied van governance, veiligheid en privacy voor alle authenticatiemiddelen en alle betrokken partijen. Ik zal ervoor zorgen dat dit verder ontwikkeld en vastgesteld wordt.
De werkzaamheden zullen parallel aan de uitvoering van de pilots opgepakt worden. Als na de pilots een beslissing tot verdere opschaling wordt genomen, wordt vervolgens door BZK periodiek getoetst of de authenticatiemiddelen voldoen aan het toelatingsstelsel.

BIT

Tijdens het Algemeen Overleg van 25 november 2015 en in een motie is gevraagd om een BIT toets te laten uitvoeren. Ik zal mijn collega van Wonen en Rijksdienst verzoeken deze toets aan het begin van de pilots te laten uitvoeren. Het Instellingsbesluit BIT[5] bepaalt de reikwijdte van de toets.

Planning

Medio 2016 zullen de uitkomsten van de pilots, van de BIT toets en van de evaluatie door Commissie Veld door het kabinet worden besproken. Tevens zal dan één set van toelatingseisen voor het publieke domein van toepassing zijn.

De ervaringen en uitkomsten van de pilots zijn essentieel voor de verdere ontwikkeling van de geteste authenticatiemiddelen, de invulling van de toelatingseisen, en de ontwikkeling van een overkoepelend toelatingsstelsel. De planning is er op gericht dat, uiteraard rekening houdend met

---

[3] Vide art. X Wet Elektronisch berichtenverkeer belastingdienst (Fi-BZK, Stb. 2015, 389), de daarop gebaseerde uitvoeringsregelgeving inzake de generieke digitale infrastructuur (GDI) en de Regeling pilot eNIk (nng).

[4] Zie brief van 19 november 2015 over pilotvoorwaarden en pilotcriteria eID Stelsel.

[5] Instellingsbesluit tijdelijk Bureau ICT-toetsing: Besluit van de Minister voor Wonen en Rijksdienst van 10 juli 2015, nr. 0000373449, tot instelling van het tijdelijk Bureau ICT-toetsing.

de uitkomsten van de pilots, in 2017 alle authenticatiemiddelen en de achterliggende partijen ten behoeve van gebruik in het publieke domein structureel binnen een overkoepelend toelatingsstelsel aan dezelfde – wettelijke – eisen voldoen op het gebied van informatieveiligheid, betrouwbaarheid en privacybescherming.
Authenticatie ten behoeve van toegang tot het publieke domein zal worden gereguleerd bij de verdere voorbereiding van de Wet GDI.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,
R.H.A. Plasterk